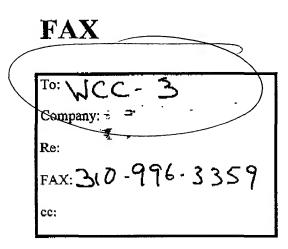
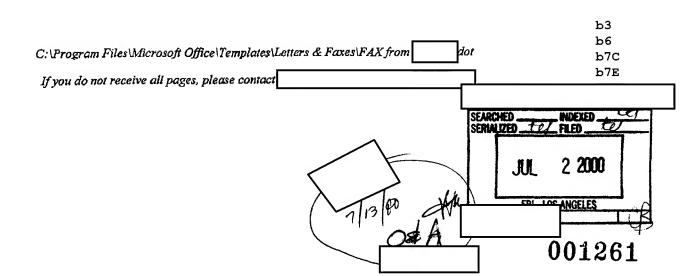
National Medical Review Offices, Inc.

5900 Wilshire Blvd., 22nd Floor Los Angeles, CA 90036



Date: 6 3 6 .2000 Number of pages including cover: 5	
From: National Medical Review Offices, Inc. 5900 Wilshire Blvd., 22nd Floor Los Angeles, CA 90036	b6 b70
Phone:	
FAX:	



b6 b7C

b6 b7C

b6 b7C

Confidential	Page 2 of 4	06/30/00
We believe that	is a clue evidencing identity o	f the hacker, because
6. An investigation of	f the breach was conducted. This r	eport was prepared
disco installed on our te	vered that passwo <u>rd cracking sections</u> security of the securi	oftware had been
Investigation of Netw	ork Security Breach, NMRO –	6/17/2000
Results of the Investi	gation	
administrative passwo passwords, they had a onto the NMRO doma mailbox using to email.	username/password. The user retains copies of his ema licious user would be able to read by are re	access to these The hacker logged cl created an email then gained access ail on the Microsoft
Chronology of Facts		
Saturday 6/17/2000		
Contacted by 6/17/2000, Someone f	rom within or outside the NMRO	g email security organization is

exchange mailboxes.

b6 b7C

b6 b7C

Confidential

Page 3 of 4

06/30/00

Monday 6/19/200

Arrived NMRO at 7:30 am and met with briefly concerning the email security incident. met with behind closed doors about the incident.
immediately began to investigate the incident. These were our
finding:
 Someone had tampered with Windows NT Users and Groups permissions on the NMRO primary domain controller other than the authorized network security personnel.
A user account that was disabled by after the individual left the company was enabled. The user was our After further investigation, several other users and groups have received domain administrator privileges not authorized by the Network Administrator Refer to the NMRO Security Update document for further reference.
2. immediately revoked Admin privileges for all unauthorized users and groups and from the NMRO domain controllers and revoked remote access privileges to the is the only NMRO employee that has remote access to the NMRO domain.

3. Focusing our attention on NMRO terminal servers, we discovered Lophtcrack 2.5 software (www.l0pht.com/l0phtcrack/) had been installed on Terminal Server (Frame 2). This software when placed and executed on a Windows NT server will crack all administrative and user passwords. A malicious hacker uses this software to gain password access in the domain. The Lophtcrack folders were deleted off the terminal servers yet the software was not removed properly from the ADD/Remove programs options in the Windows NT control Panel. Therefore leaving a trail that the software was loaded on the server.

Confidential

Page 4 of 4

06/30/00

4. Upon further investigation Lophtcrack 2.5 was brought into the organization by our	b6 b7С
END OF REPORT	
Please call me, or as soon as possible. Thank you in advance for your attention to this matter.	ь6 ь7с
Sincerely	

FEDERAL BUREAU OF INVESTIGATION

	Date of transcription	07/19/2000
inter provi	was interviewed telephonical. After being advised of the official identification in the purpose of the interview, identification:	
event of th June	is employed by National Medical Report of 2000. Is employed by National Medical Report of 2000. Is employed by National Medical Report of 2000. Is employed by National Medical Report of 2008 and security logs in an attempt to identify a specific consible for these intrusions.	ined NMRO's the origin April and
accou Acces appro remot had h of th	access to NMRO's system was or his termination. subsequently examined ants of a number of people who are no longer employes to these accounts should have been disabled. He eximately 06/15/2000, found that the passe logon capabilities for approximately six of these een enabled. This included account. See had administrative privileges. These accounts are been enabled from inside the company. However, icult to determine how and when these accounts were	d the yed by NMRO. owever, on swords and se accounts The majority would have, it is
went days.	There were several instances between the mide and June, 2000 when NMRO's system had suspicious of down. The system was down for a total of approximate approximate suspected that someone was hacking into an attempt to shut it down.	outages and mately three
the s	The affected machine was NMRO's mail server. Ider may have gained access through a program or beserver. Server. and would have bettunity to install such a program on that server.	atch file on
crack told	LOPHT is a hacker group that does not engage rity. This group created a program called LOPHTCRASS system passwords. Into run this program on NMRO's system in the system.	ACKER that
gation on	07/13/2000 at Los Angeles, California (teler	honically)
	Date dictated 07/19/	2000
C3 [

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b3

b6 b7C b7E

b6 b7C

b6 b7C

To: NSD From: Los Logeles Re:, Date 07/20/2000
these accounts had been enabled. This included account. The majority of these had administrative privileges. These accounts would have to have been enabled from inside the company. However, it is difficult to determine how and when these accounts were enabled.
There were several instances between the middle of April, 2000 and June, 2000 when NMRO's system had suspicious outages and went down. The system was down for a total of approximately three days. suspected that someone was hacking into NMRO's system in an attempt to shut it down.
The affected machine was NMRO's mail server. The intruder may have gained access through a program or batch file on the server. and would have had ample opportunity to install such a program on that server.
LOPHT is a hacker group that does not engage in criminal activity. This group created a program called LOPHTCRACKER that cracks system passwords. In
of NMRO's servers which are main domain controllers are named The Internet Protocol (IP) addresses for these servers are respectively.
Given that there has not been a verifiable financial

b3 b6 b7C b7E

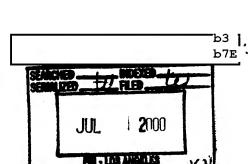
> b6 b7C b7E

loss to NMRO or theft of trade secrets, and because the intrusions are not ongoing, writer recommends that case be opened and closed. Investigation at Los Angeles complete.

	b3
	b6
(Title)	b7C
	b7E
(File No.)	

Item	Date Filed	To be returned Yes No		Disposition
1	7-31-00		notes re'	tel
<u> </u>		<u> </u>		
		i		
		İ		





*11/2 ml Contract

(experted value Mul to end 4/00 - prote ~ 6/15 - noticed Thompsell 2-12/2 weeks after left to when deloved and. Mand server affect; fysgested - No commonds mortes songund or lath fighe Junes;
That softways CAPHT - Clean haus group - Ino of the peop COPHT CRACKER for PUTS -Told that he had that prong told to run it to text to to run it to test to Loguerde available Comp born- Would have loop Devel include from mile 4/2000 po mul 6/2000, Dusquour devays -down, 3dag